

Safety is the cornerstone upon which we build mission success.

PRA Role in System Safety and Continuous Risk Management

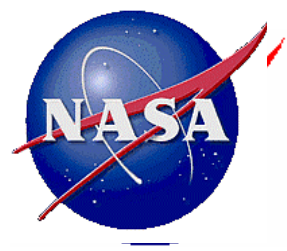
Homayoon Dezfuli, Ph.D.
Manager, System Safety
Office of Safety and Mission Assurance
NASA HQ
hdezfuli@nasa.gov (202) 358-2174



Safety is the cornerstone upon which we build mission success.

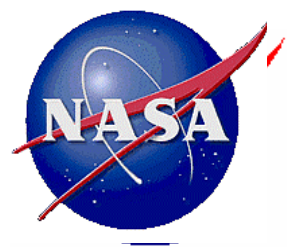
CAIB Report Finding F7.4-4 (Volume I, page 193)

“System safety engineering and management is separated from mainstream engineering, is not vigorous enough to have an impact on system design, and is hidden in the other safety disciplines at NASA Headquarters.”



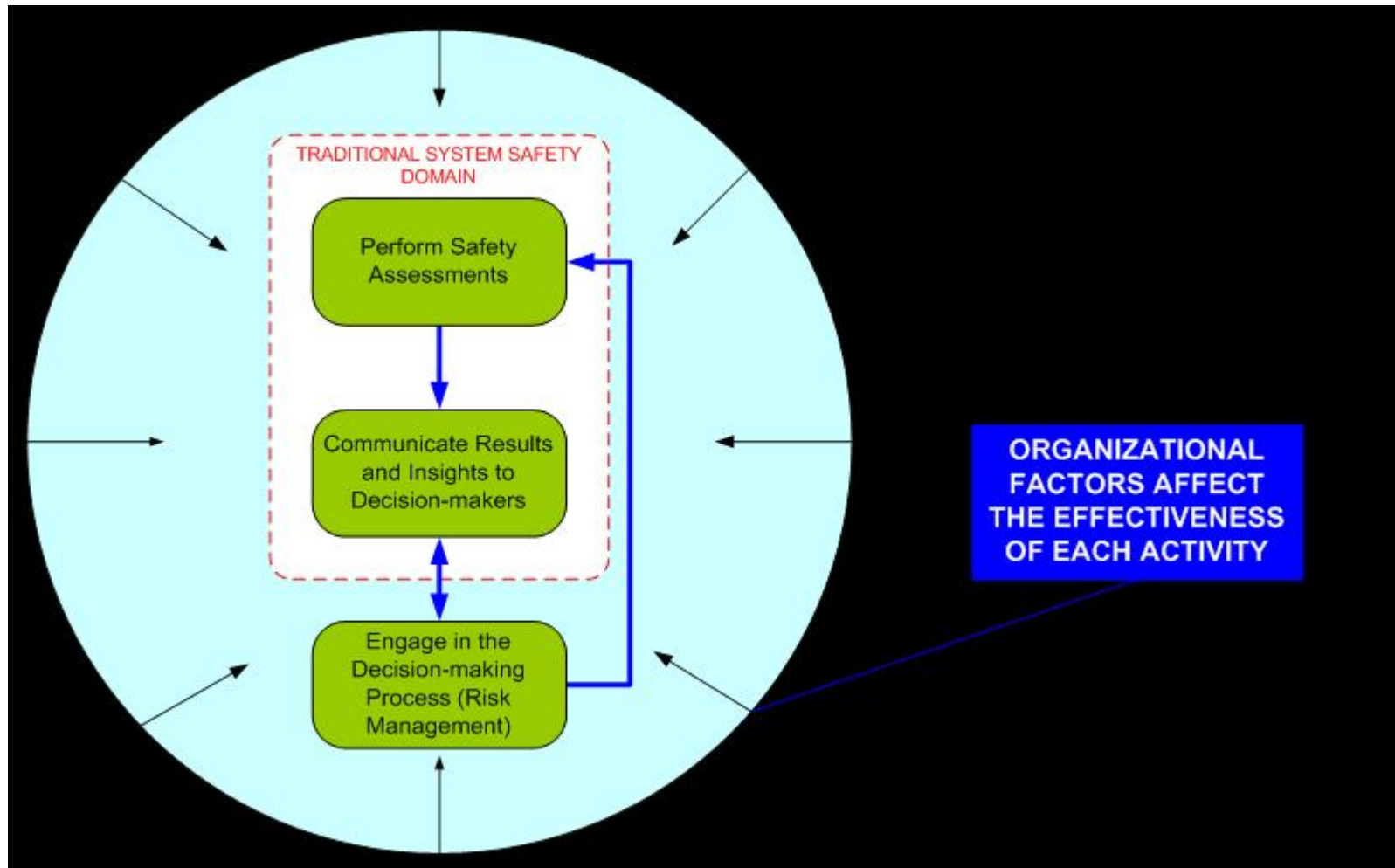
Objectives of the System Safety

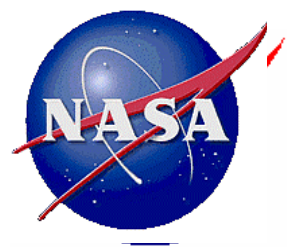
- To prevent injury to personnel, loss of or damage to property, loss of technical stature, or environmental harm. *NPR 8715.3, paragraph 1.3*
- To provide for an organized, disciplined approach to the early identification and resolution of risks impacting personnel, hardware, or mission success to a level that is as low as reasonably achievable. *NPR 8715.3, para 3.3*
- How: *NPR 8715.3, para 1.3.6*
 - Assessments of both qualitative and quantitative safety risks to people or property
 - Means: “PERFORM ASSESSMENTS”
 - along with recommendations to either reduce the risks or accept them
 - Means: “ENGAGE IN DECISION-MAKING”



Safety is the cornerstone upon which we build mission success.

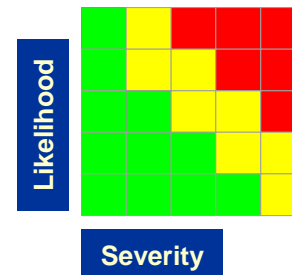
Key Activities of the System Safety Process

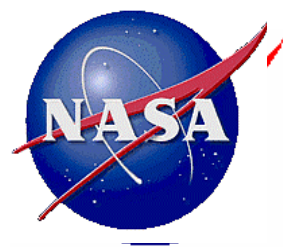




Traditional System Safety Assessment Techniques

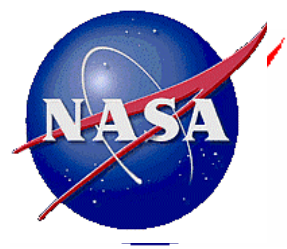
- Analyst postulates a failure or a deviation and assesses its consequences
 - Typically one failure or deviation is analyzed at a time
- Analyst qualitatively judges how often a failure or deviation can occur
- Analyst qualitatively judges the severity of the outcome or assumes the worst-case outcome
- Instead of systematically quantifying risk, analyst maps each analyzed failure into one of three risk categories (Green, Yellow, Red)





Proposed enhancements to system safety practices at NASA

- **Do more effective assessments**
 - Orient system safety assessments toward mission objectives
 - Incorporate probabilistic risk assessment (PRA) techniques into Traditional System Assessments
 - Use peer review process to improve the quality of system safety assessments
- **Communicate more effectively**
 - Provide context to help the decision-makers evaluate the implications of safety findings
 - Explicitly evaluate uncertainties in the assessments
- **Engage in the decision-making process**
 - Coordinate and collaborate with other stakeholders to manage risk



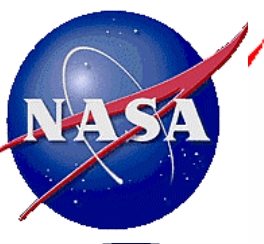
Orienting System Safety Assessments Toward Mission Safety

- **A mission-oriented approach to system safety should be employed**
 - **Provides focus for safety assessments**
 - Steers safety assessments toward the fundamental objectives of the mission (big picture)
 - Eliminates stove-piped safety assessments
 - **Promotes integration and coordination of safety assessments**
 - Captures systems interactions in safety assessments
 - Promotes integration of safety assessments with other assessments
 - Cost
 - Schedule
 - **Fosters better communication of safety issues**
 - Helps the decision-makers to appreciate the significance of safety issues in terms of the big picture



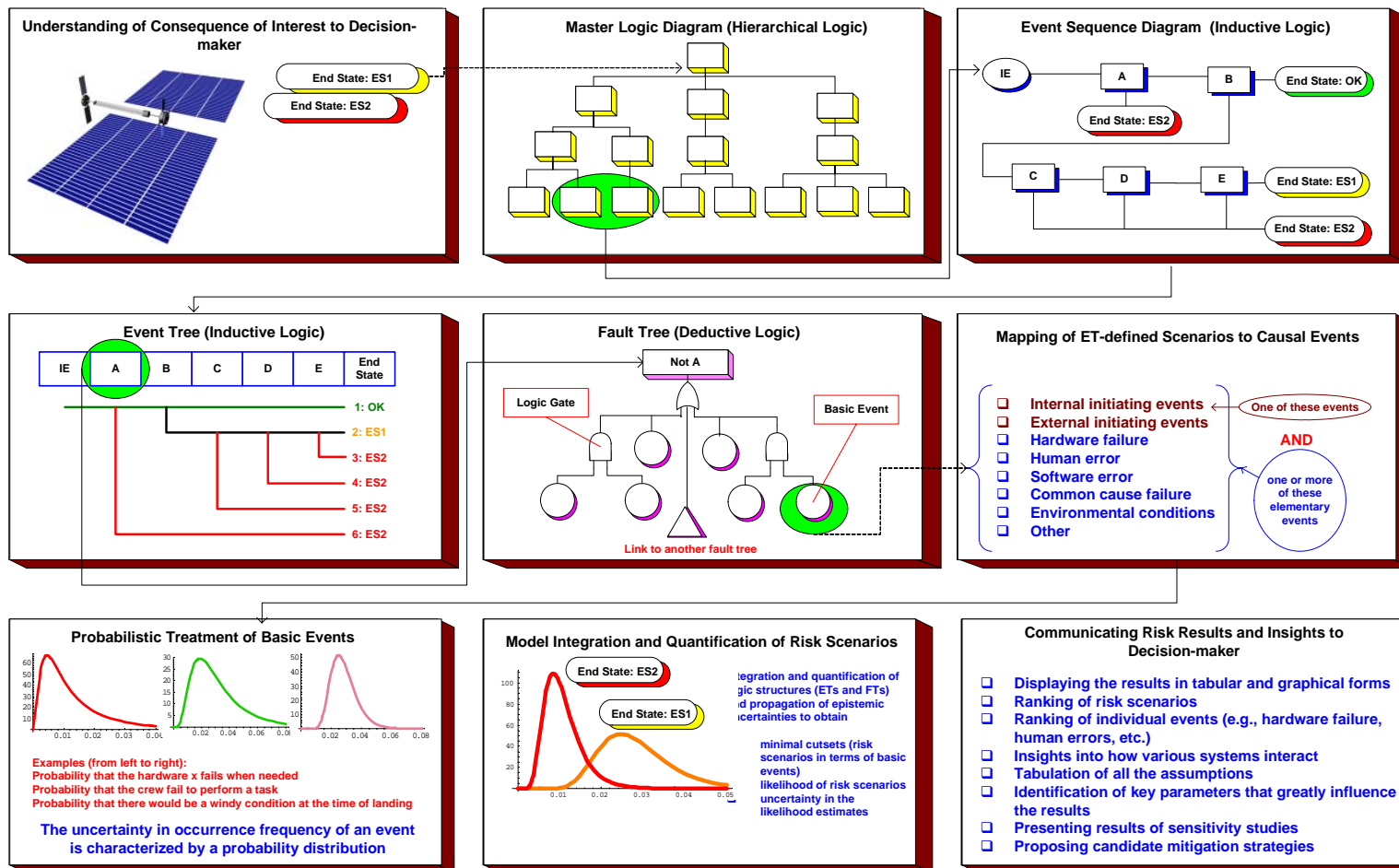
Incorporation of PRA Techniques into Traditional System Assessments

- **PRA should be used whenever possible to complement qualitative assessment of hazards.**
 - Traditional system safety analyses (hazard analysis, fault tree analysis, and FMEA) are to be integrated into a coherent assessment process
- **PRA has been shown to be a useful tool to quantify risk metrics relating to the likelihood and severity of events adverse to safety or mission success**
 - Identifies a complete set of credible system failure modes
 - Captures interactions between events/systems/crews in an integrated modeling framework
 - Quantifies uncertainties and identifies what the system safety analysts know or do not know
 - Facilitates decision-making by identifying the dominant risk contributors, so that risk management decisions are targeted toward risk significant hazards



Safety is the cornerstone upon which we build mission success.

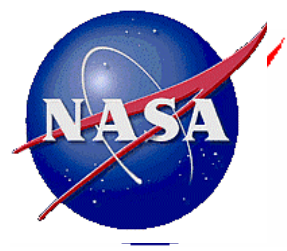
PRA Process





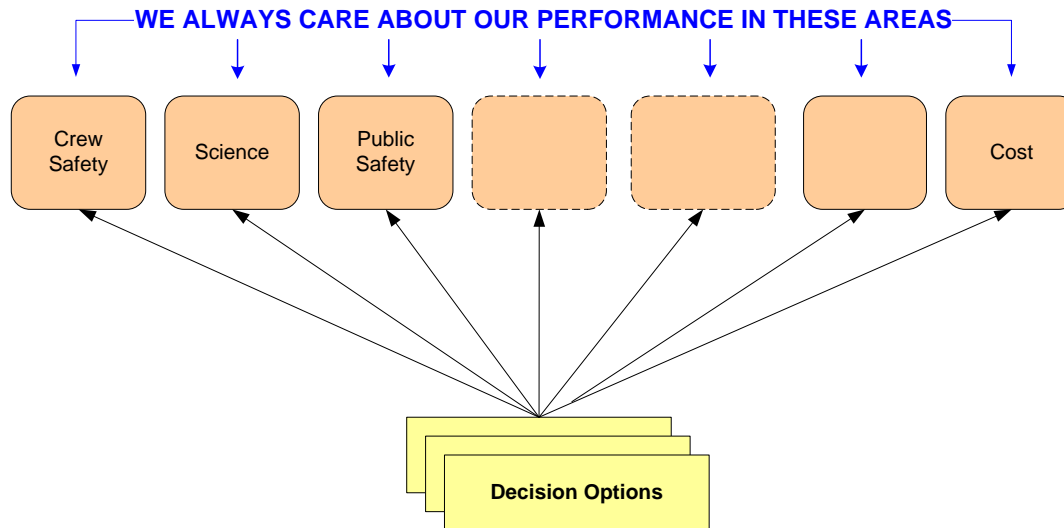
Need for Effective Communication of Safety Issues

- **Risk communication provides the link between system safety assessments and risk management**
 - The analyst should clearly identify what he/she knows or does not know
 - Clear and concise tabulation of all known limitations and constraints associated with the assessment
 - Identification of key assumptions that greatly influence the results of the assessment
 - The analyst should always present results in the context of the big picture (i.e., mission objectives)
- **Credibility is the key for influencing the decision-makers**
 - A clear presentation of the uses, limitations, and uncertainties of the assessment



Safety is the cornerstone upon which we build mission success.

Our Decisions Influence and are Influenced by Many Factors

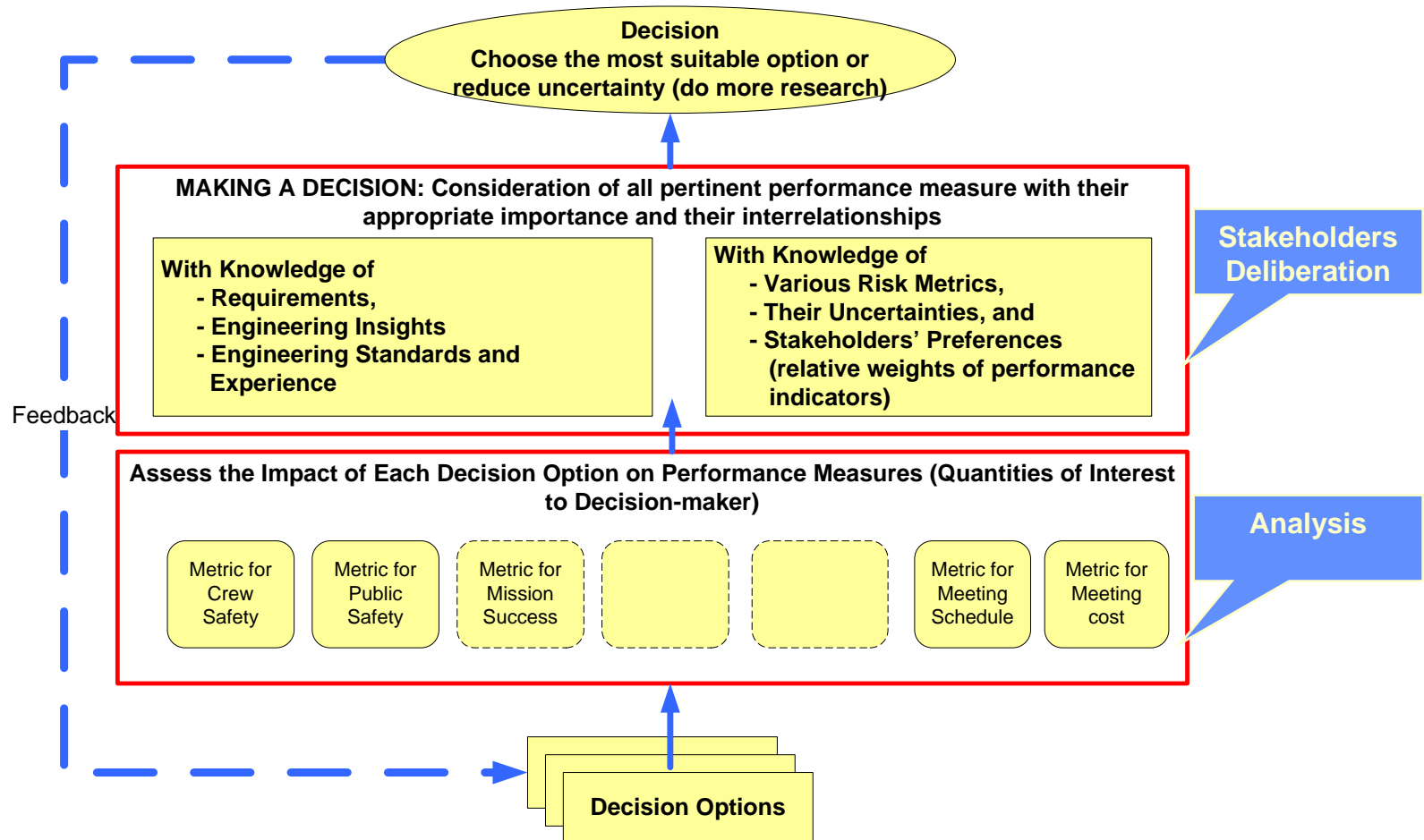


Decision situations

- Designing new systems.
- Making changes to existing systems.
- Extending the life of existing systems.
- Changing requirements.
- Responding to mishaps in real time.
- Allocating resources.
- Initiating research programs to reduce uncertainty.
- Other

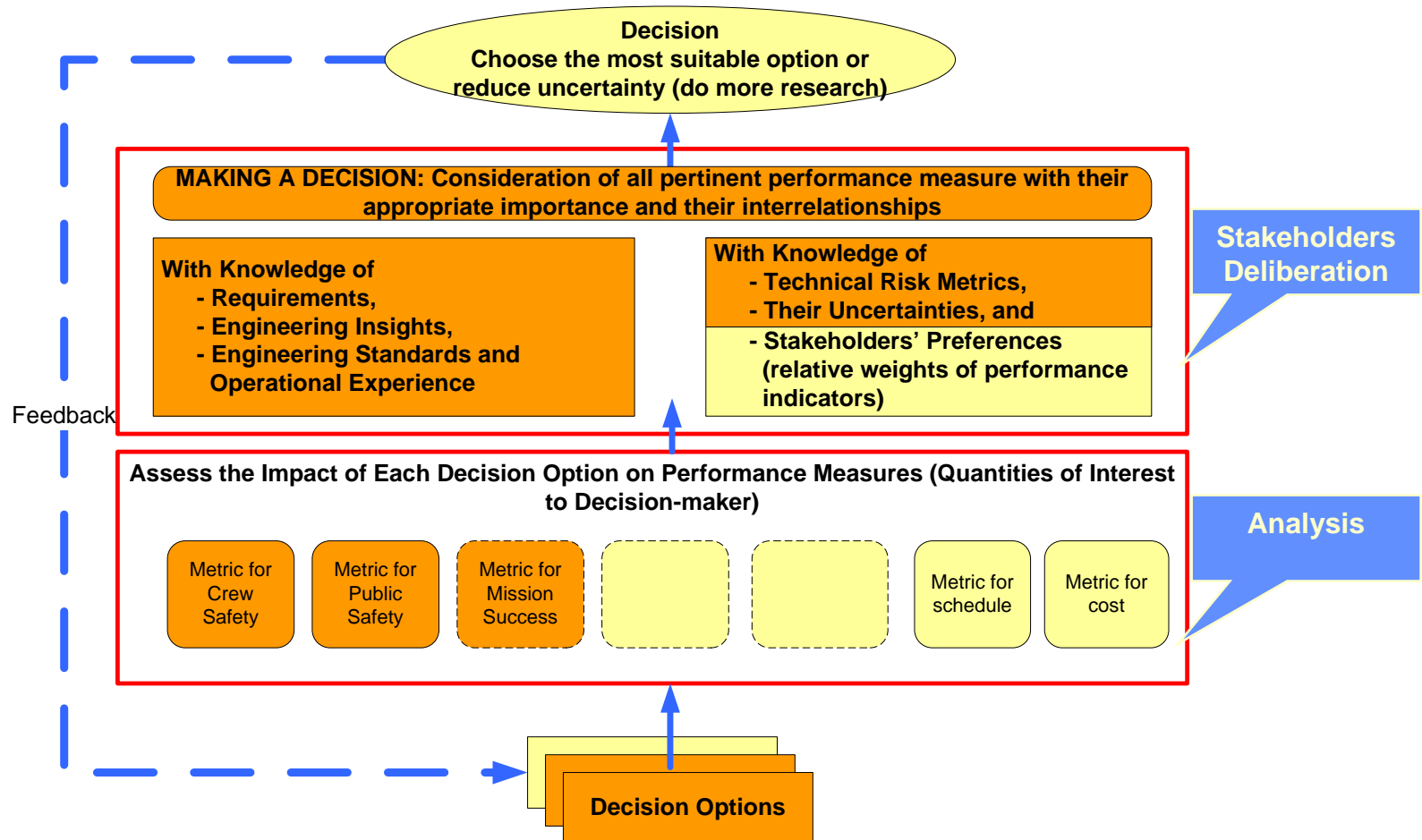


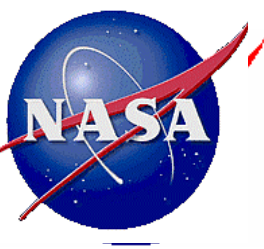
A Risk-informed Decision-making Framework





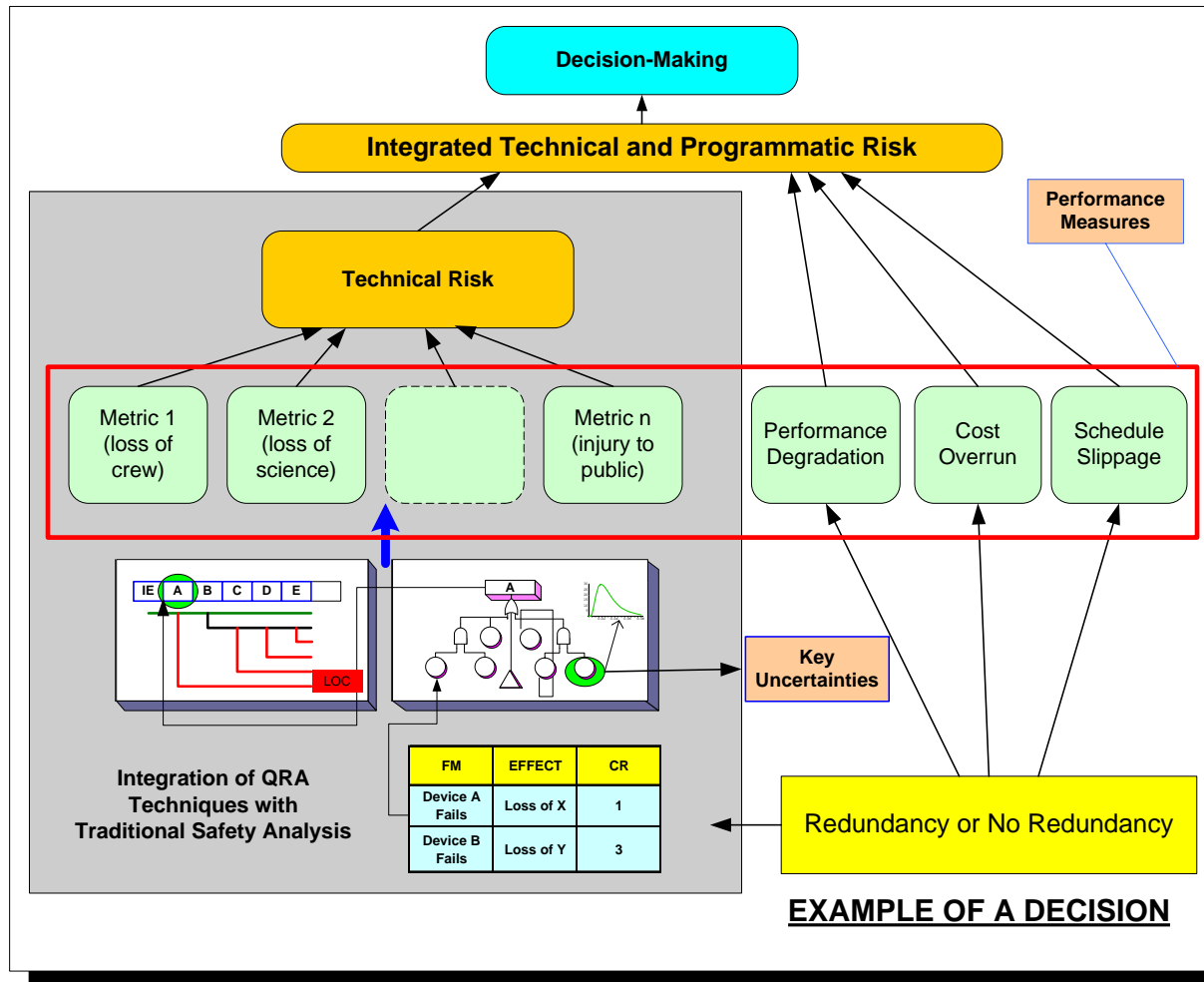
System Safety Involvement in Decision-making

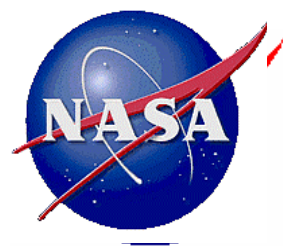




Safety is the cornerstone upon which we build mission success.

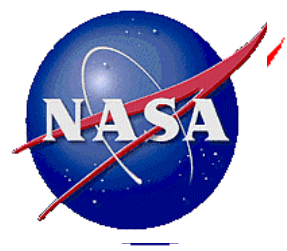
Integration of Quantitative Risk Assessment with Traditional System Safety Analyses





How Risk-informed Decision-making Works

- **Consequences of decision options are modeled in terms of the performance measures (PM) relating to the program fundamental objectives**
 - PMs are attributes or their surrogates that are measurable
 - Example: PM for crew safety can be the probability of loss of crew
 - Example: PM for ELV performance can include capability and reliability
- **Preferences (relative weights of key performance measures) are obtained from each stakeholder**
 - Incorporating the stakeholders' views into the decision-making process
- **Decision options are ranked according to their desirability**
 - Comparing the consequences of decision options on the PMs
- **The most suitable decision option is selected through deliberations amongst stakeholders**
 - Deliberation is any formal or informal process for communication and collective consideration of issues



NASA is Moving to a Risk-informed Decision-making Environment

- **NASA's 2003 Strategic Plan States:**

“Decision-making in the face of uncertainties that affect cost, schedule, and technical parameters demands that our managers understand the impact of trade-offs on the potential for program success. Our managers must have the information and training they need to make well-informed decisions, and our stakeholders must be able to see how we arrive at key missions decisions. We must develop modern tools for cost and risk analysis.” Page A-3: Implementation Strategy 5

- **Incorporating System Safety activities in a risk-informed decision-making framework is required according to the Agency's strategic plan**



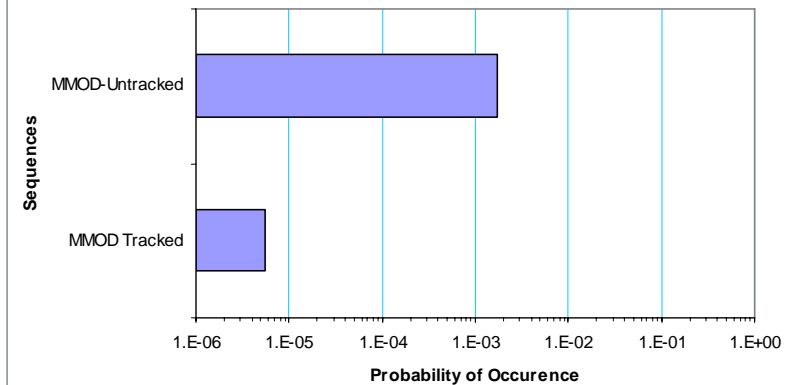
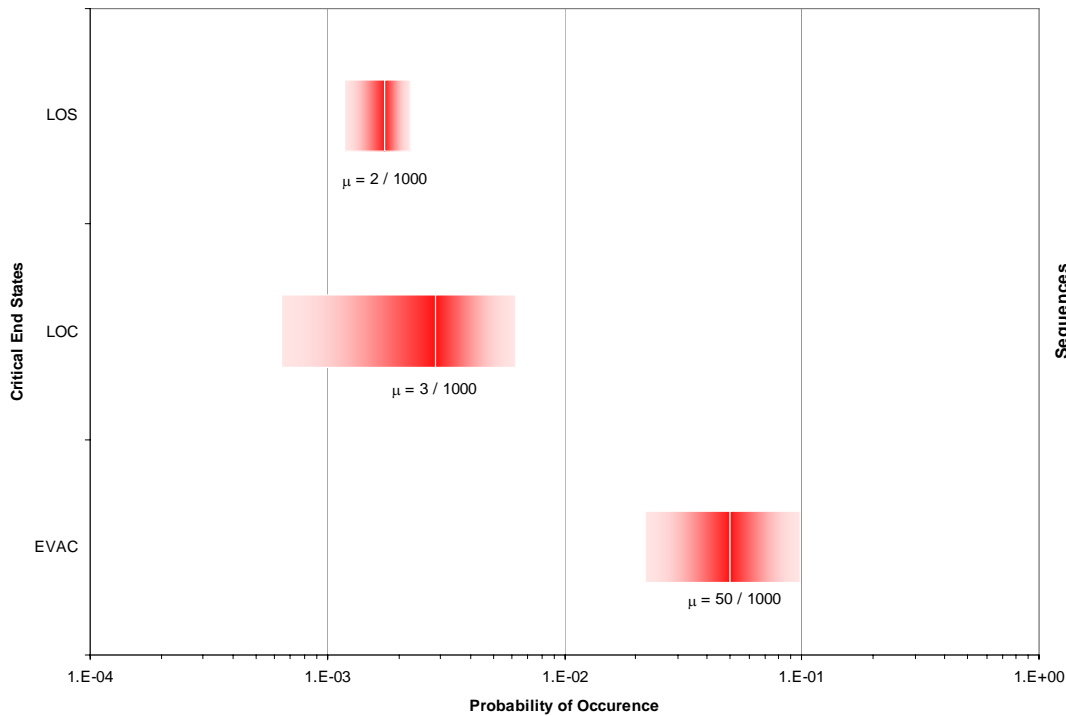
How Risk-informed Decision-making Works

- **Consequences of decision options are modeled in terms of the performance measures (PM) relating to the program fundamental objectives**
 - PMs are attributes or their surrogates that are measurable
 - Example: PM for crew safety can be the probability of loss of crew
 - Example: PM for ELV performance can include capability and reliability
- **Preferences (relative weights of key performance measures) are obtained from each stakeholder**
 - Incorporating the stakeholders' views into the decision-making process
- **Decision options are ranked according to their desirability**
 - Comparing the consequences of decision options on the PMs
- **The most suitable decision option is selected through deliberations amongst stakeholders**
 - Deliberation is any formal or informal process for communication and collective consideration of issues



Safety is the cornerstone upon which we build mission success.

Representative QRA Results (International Space Station Probabilistic Risk Assessment; Phase II, Stage 7A)



LOS: Loss of Station
LOC: Loss of Crew
EVAC: Evacuation
MMOD: Micrometeoroids and Orbital Debris